Abstract of the Disclosure

Let us consider a message M an element $(m1,m2, \cdots,mk)$ in a Galois field $GF(2^k)$, and multiply it by a product of polynomials $\beta\ 1(\alpha)$- $\beta\ t(\alpha)$ into $M(\alpha)$.

$$M(\alpha) = M\beta\ 1(\alpha) \cdot M\beta\ 2(\alpha) \cdot \cdots \cdot M\beta\ t(\alpha)$$

Combine a noise vector $r(\alpha)$ of n - k to $M(\alpha)$ in series so that the data is expanded into degree n. Next, they are transformed into Γ by permutation. Γ is multiplied by an element γ^{x} in the Galois field $GF(2^n)$ into cyphertext C(M), where γ is a primitive root of the multiplicative group of the Galois field $GF(2^n)$. Practically, when the message M is substituted for X in a public key C(X), the cyphertext C(M) is obtained. The cyphertext C(M) is multiplied by γ^{-x}, is applied to an inverse permutation, and the noise vector $r(\alpha)$ is separated. Then, the inverse element of the product of $\beta\ 1(\alpha) - \beta\ t(\alpha)$ is multiplied and is raised to an adequate index. Then the decrypted message is obtained.